Rendu de documentation sur le projet de mise en place d'Active Directory avec autorisations sélectives

Partie 1 : Veille technologique

I. Introduction

Dans le cadre de ce projet, notre objectif était de mettre en place un environnement Active Directory avec des autorisations sélectives en fonction des métiers, des types de comptes et des opérations. Cette documentation présente en détail notre démarche de réalisation, les recherches effectuées pour la veille technologique, les choix techniques, ainsi que les contraintes et limites rencontrées tout au long du projet.

II. Contexte technologique et veille

Avant de débuter le projet, nous avons effectué une veille technologique approfondie sur Active Directory, Windows Server et les meilleures pratiques en matière de gestion des identités et des accès. Nous avons étudié les fonctionnalités, les avantages et les inconvénients d'Active Directory, ainsi que les différentes méthodes pour configurer des autorisations sélectives.
Un site qui nous a permis de bien comprendre le projet est :

1. IT-Connect - Site web spécialisé en technologies de l'information : Ce site web fournit des informations détaillées sur divers sujets techniques, y compris Active Directory, Windows Server et la gestion des identités et des accès. Nous avons consulté ce site pour approfondir nos connaissances et obtenir des informations pratiques sur la mise en place d'Active Directory avec des autorisations sélectives. Cette veille nous a permis de comprendre les fondements théoriques et pratiques nécessaires à la réalisation du projet.

III. Outils, paquets et services installés

Pour la mise en place de notre environnement, nous avons utilisé les outils et services suivants :

1. Windows Server : Nous avons installé Windows Server comme système d'exploitation serveur principal.
2. VirtualBox : Nous avons utilisé cette plateforme de virtualisation pour créer nos machines virtuelles (VMs) et installer Windows Server.
3. Active Directory : Nous avons activé et configuré Active Directory en tant que service de gestion des identités et des accès.
4. Matrice PAM : Nous avons créé une matrice qui traduit les permissions de groupes en fonction des niveaux de droits requis pour chaque catégorie d'utilisateurs.
5. Schéma d'architecture : Nous avons élaboré un schéma d'architecture qui différencie les différents niveaux, notamment l'infrastructure, les serveurs et les services.

IV. Choix techniques

Lors de la mise en place de notre environnement Active Directory, nous avons pris les décisions techniques suivantes :

1. Utilisation de Windows Server 2022 : Nous avons choisi d'utiliser Windows Server en raison de sa compatibilité avec Active Directory et de sa robustesse en tant que système d'exploitation serveur.
2. Virtualisation : Nous avons opté pour la virtualisation des serveurs à l'aide de VirtualBox pour faciliter la gestion des environnements de test.
3. Gestion des utilisateurs et des groupes : Nous avons utilisé les fonctionnalités intégrées d'Active Directory pour créer et gérer les utilisateurs, les groupes et les autorisations.

4. Utilisation de Windows 10 pro : Nous avons choisi ce système d'exploitation pour les ordinateurs de notre domaine.

V. Contraintes et limites rencontrées

Pendant la réalisation du projet, nous avons fait face à certaines contraintes et limites, notamment :

1. Limitations matérielles : Nous avons dû nous assurer d'avoir suffisamment de ressources matérielles pour exécuter les machines virtuelles et les services nécessaires.
2. Complexité de la configuration initiale : La configuration initiale d'Active Directory peut être complexe, notamment la mise en place des relations de confiance, des stratégies de groupe, etc. Nous avons dû consacrer du temps à la compréhension approfondie de ces aspects.
3. Besoins de sécurité : Nous avons dû prendre en compte les besoins de sécurité, notamment en ce qui concerne la gestion des mots de passe, l'accès aux données sensibles, etc.

VI. Tests de conformité

Avant de mettre en service notre solution, nous avons effectué plusieurs tests de conformité pour valider son bon fonctionnement. Les tests comprenaient :

1. Vérification des autorisations : Nous avons vérifié que les utilisateurs étaient correctement assignés à leurs groupes respectifs et que les autorisations accordées étaient conformes à la matrice PAM.
2. Tests d'accès aux ressources : Nous avons effectué des tests d'accès aux ressources pour s'assurer que les utilisateurs peuvent accéder uniquement aux ressources qui leur étaient autorisées.
3. Tests de réplication : Nous avons vérifié que la réplication des données d'Active Directory fonctionnait correctement entre les contrôleurs de domaine.

VII. Conclusion de notre veille technologique

En conclusion, la mise en place de l'environnement Active Directory avec des autorisations sélectives a été réalisée avec succès. Grâce à une veille technologique approfondie, des choix techniques adaptés et des tests de conformité rigoureux, nous avons pu mettre en place une solution fonctionnelle et sécurisée pour la gestion des identités et des accès au sein de notre environnement.

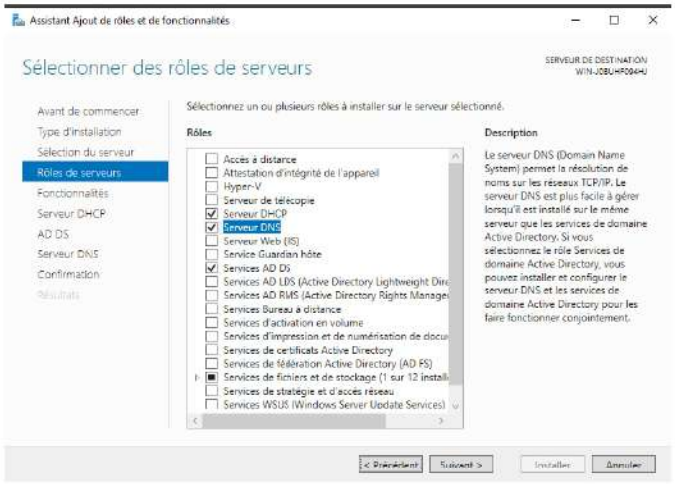
Partie 2 : Configuration

1. Configuration IP

Dans “Panneau de configuration”, dans “Réseau et Internet”, dans “Centre Réseau et partage”. Cliquez sur la carte réseau qui vous intéresse. Si elle n’apparaît pas, aller dans “Modifier les paramètres de la carte”. Une fois dans le menu de votre carte réseau, allez dans “Propriétés”, décocher “Protocole Internet version 6 (TCP/IPv6)” si vous n’en avez pas l'utilité. Allez dans “Protocole Internet version 4 (TCP/IPv4)”, passez en mode manuel, précisez l’IP que vous souhaitez et le ou les DNS dont vous souhaitez vous servir.

2. Configuration DHCP

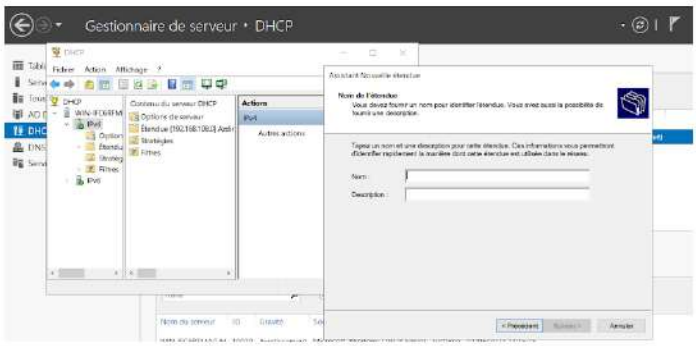
Sur Windows Server, sur la page d'accueil du gestionnaire de serveur, il faut "Ajouter des fonctionnalités”, suivre les instructions et cocher la case "Serveur DHCP".

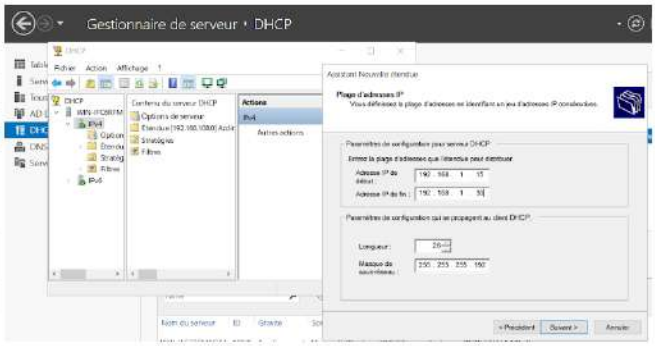


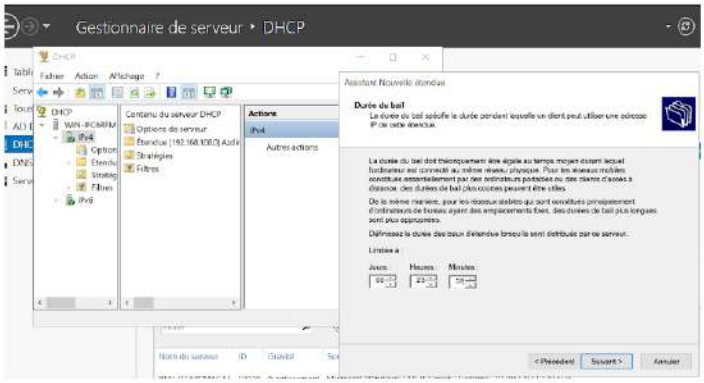
Quand l'installation est terminée, un chiffre orange apparaît au niveau du drapeau à droite dans le gestionnaire de serveur, lorsqu’on clique dessus, on se laisse guider. Maintenant on peut passer à la configuration. Dans le "Gestionnaire DHCP", ajouter une "Nouvelle étendue" en lui donnant un nom (peu importe), une durée de validité pour l'adresse IP(bail). Préciser l'adresse IP de début et celle de fin (192.168.1.15 et 192.168.1.30 par exemple).

Le masque de sous-réseau se met automatiquement. Toutefois selon notre besoin on peut le modifier à notre guise. On peut préciser une passerelle par défaut. Pour les serveurs DNS, nous avons ajouté les adresses IP 8.8.8.8 pour Google et 1.1.1.1 pour un serveur DNS rapide et sécurisé. On peut aussi spécifier des adresses IP à exclure de notre plage (afin de les attribuer à des machines spécifiques, par exemple).

Après cette configuration, le serveur DHCP distribuera de manière automatique les adresses IP en fonction.







3. Configuration DNS

Nous ne l'avons pas fait, car nous nous sommes aperçus après plusieurs tentatives, qu'il se configurait automatiquement.

4. Configuration AD

Comme pour le DHCP, dans Windows Server, il faut "Ajouter des fonctionnalités", et cocher la case "AD DS".
Quand l'installation est terminée, dans l'assistant Configuration des services de domaine AD, dans "Configuration de déploiement", choisir "Ajouter une nouvelle forêt" et spécifier le nom de domaine racine (active.directory.local par exemple). Il faut ensuite cliquer "Promouvoir ce serveur en contrôleur de domaine" puis "Ajouter un contrôleur de domaine à un domaine existant".
Suivre les instructions de l'assistant pour la promotion du serveur pour paramétrer la configuration avec le nom de domaine, l'identification de l'administrateur, les options pour la réplication, le stockage des données, etc. Les paramètres de sécurité avec les mots de passe complexes, le verrouillage de compte, etc.
Après avoir terminé avec l'assistant, il faut redémarrer pour finaliser la promotion du serveur au rôle de contrôleur de domaine.
Il faut configurer les privilèges et les accès avec les outils AD comme "Utilisateurs et ordinateurs AD". Créer des groupes d'utilisateurs, leur définir des droits et des autorisations en fonction de la matrice PAM.

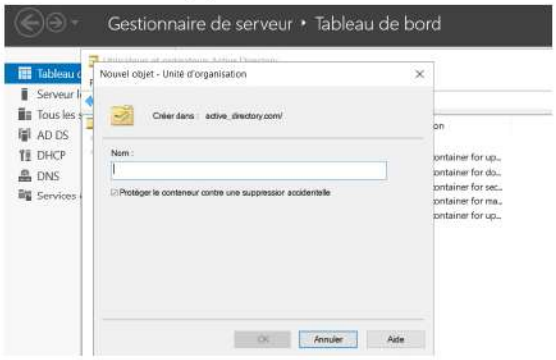
5. Ajout des utilisateurs

Matrice PAM :

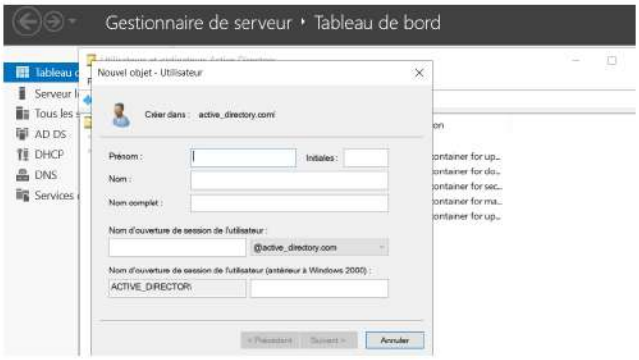
Rôles	Catégorie	Versements inférieur ou égal à 10 000 €	Versements inférieur ou égal à 100 000 €	Versements supérieur à 100 000 €	Accès au compte
guichetiers	A	Lecture	Lecture	Lecture	
conseillers de clientèle privés	B	Lecture/ écriture	Lecture	Lecture	Lecture/ écriture
gestionnaires et conseillers de clientèle pro	C	Lecture/ écriture	Lecture et si demande écriture	Lecture	Lecture/ écriture
personnel dirigeant	D	Lecture/ écriture	Lecture/ écriture	Lecture/ écriture	Lecture/ écriture
Clients de la banque					Lecture
Informaticiens et prestataires		Lire/ exécuter	Lire/ exécuter	Lire/ exécuter	Lire/ exécuter
Chef de projet		Lire/ écriture/ exécuter	Lire/ écriture/ exécuter	Lire/ écriture/ exécuter	Lire/ écriture/ exécuter

Pour des raisons de sécurité il est préférable de désactiver le compte administrateur et de créer un ou plusieurs utilisateurs qui auront des privilèges similaires.
Pour ajouter des utilisateurs il faut d'abord créer une unité d'organisation (OU) qui permet d'organiser et gérer les objets, comme les utilisateurs, les groupes et les ordinateurs au sein d'une structure hiérarchique.

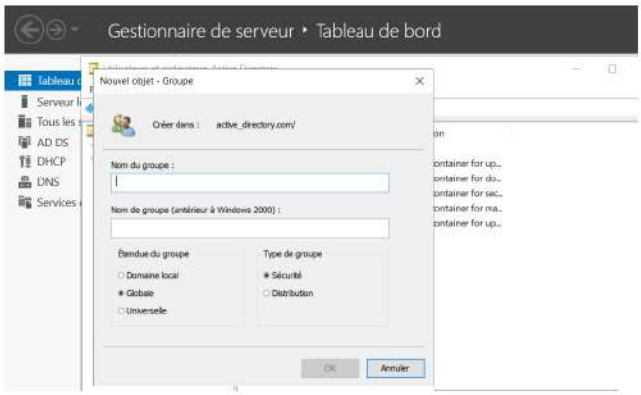
Dans le contrôleur de domaine, ouvrir "Utilisateurs et ordinateurs AD" et choisir l'emplacement où placer la nouvelle OU. Choisir "Nouvelle unité d'organisation" dans le menu, choisir un nom approprié et OK. La nouvelle OU apparaît dans l'arborescence d'AD.



Choisir ensuite "Nouvel utilisateur" et suivre les instructions de l'assistant. Donner le prénom et le nom de l'utilisateur, son nom d'ouverture de session unique (sAMAccountName) qui sera utilisé pour l'authentification. Son mot de passe que l'utilisateur pourra changer lors de sa première connexion. Possibilité de déterminer une durée de validité du mot de passe, l'expiration du compte entre autres. Avec "Terminer", l'utilisateur est créé.



Choisir ensuite "Nouveau groupe" et suivre les instructions de l'assistant. Donner le nom du groupe. Avec "OK", le groupe est créé.



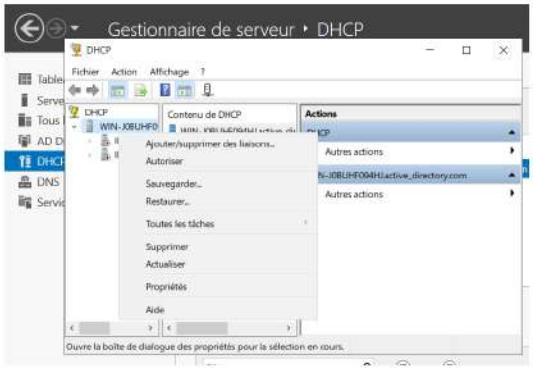
On peut maintenant ajouter les utilisateurs dans un groupe. Pour cela, on peut soit dans le menu de l'utilisateur lui attribuer un ou plusieurs groupes, soit depuis un groupe en lui attribuant un ou plusieurs utilisateurs.

On peut aussi ajouter un groupe ou un utilisateur à l'aide de script powershell.

6. Reconfiguration DHCP

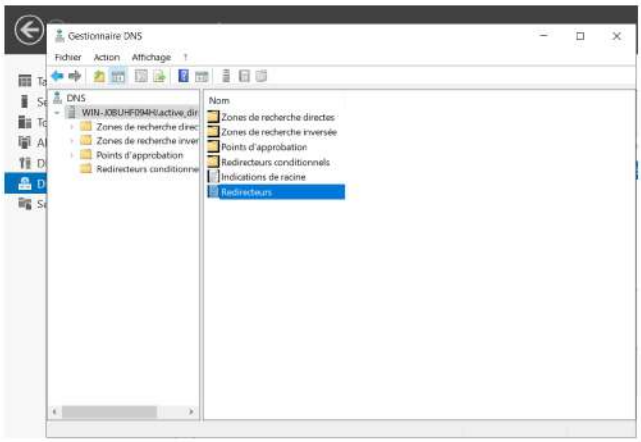
Autoriser

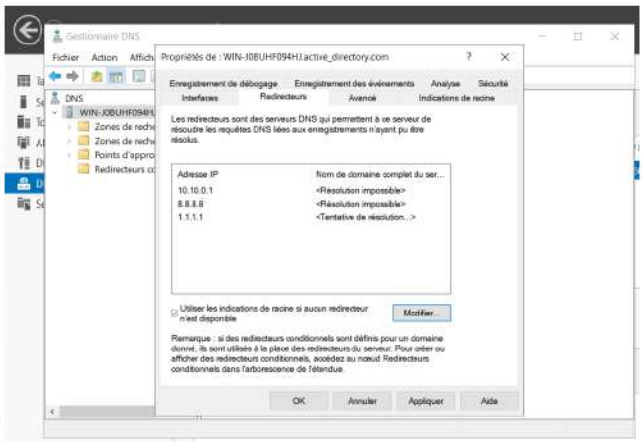
Dans le Gestionnaire de serveur, aller sur "DHCP" dans la liste des rôles.
Ensuite, dans la fenêtre du Gestionnaire DHCP, cliquez avec le bouton droit de la souris sur votre serveur DHCP et sélectionnez "Autoriser" pour activer le service DHCP avec le serveur AD.



7. Ajout des redirecteurs du serveur DNS

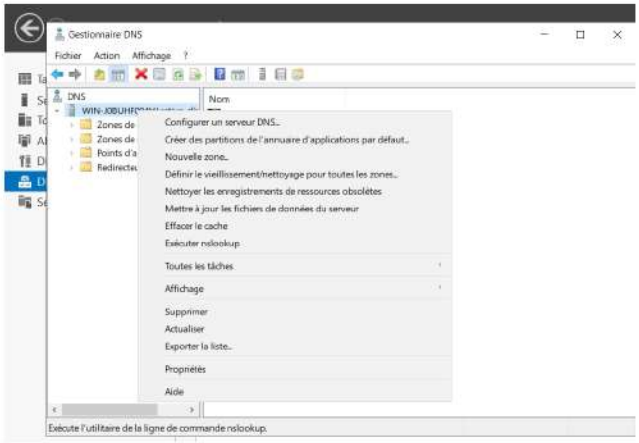
Comme on a fait le choix de ne pas configurer le serveur DNS auparavant, il faut maintenant ajouter des redirecteurs qui correspondent à d'autres serveurs DNS. Ce qui permettra à notre serveur de pouvoir utiliser plusieurs DNS et ainsi améliorer ses performances.





8. Mise à jour du serveur DNS

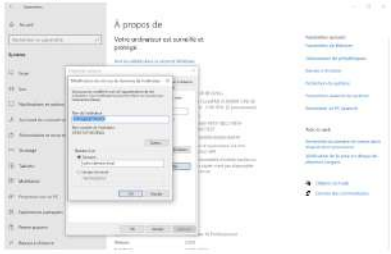
Ensuite il faut mettre à jour le serveur DNS



9. Intégrer un PC dans un domaine

Prérequis : le PC doit disposer d'une connexion réseau fonctionnelle et doit pouvoir accéder au contrôleur de domaine.

Dans les paramètres, aller dans “système”, puis dans “à propos de”.
Dans "Renommer ce PC (avancé)".
Il faut entrer dans “membre d’un domaine” le nom de domaine de l’AD. Si tout fonctionne, une fenêtre apparaît nous invitant à rentrer les identifiants de connexions d’un administrateur du domaine Active Directory. Une fois validé, redémarrer le PC pour appliquer les modifications.
Rechercher le nom du PC dans la liste des objets et le PC devrait y apparaître. Avec un clic droit choisir "Propriétés" et vérifier les informations (nom, adresse IP, etc).



10. Dossiers partagés

La gestion des dossiers partagés est une fonctionnalité essentielle dans un environnement de réseau. Les dossiers partagés permettent aux utilisateurs d'accéder, de partager et de collaborer sur des fichiers et des ressources de manière centralisée. La configuration des dossiers partagés peut être réalisée en utilisant la Gestion de stratégie de groupe (GPO) dans un environnement Windows.

Partager un dossier par le Gestionnaire de serveur :

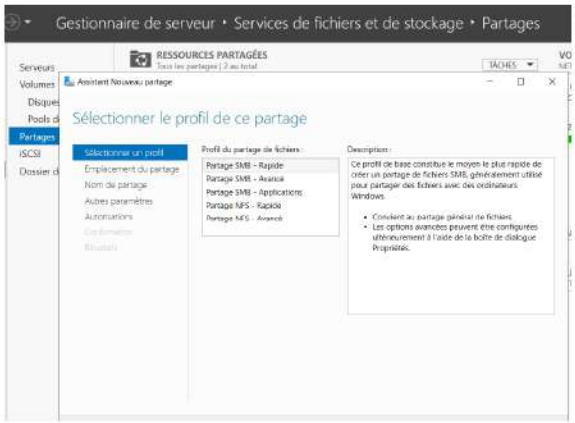
Pour partager un dossier en utilisant le Gestionnaire de serveur, vous devez tout d'abord ouvrir le Gestionnaire de serveur et accéder à la gestion des partages dans la section "Services de fichiers et de stockage". Ensuite, vous cliquez sur "TÂCHES" ou faites un clic droit et sélectionnez "Nouveau partage" pour lancer l'assistant.

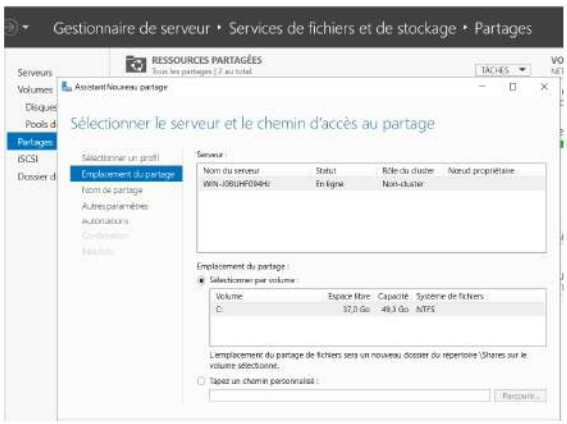
Dans l'assistant, choisissez le profil "Partage SMB - Rapide" et cliquez sur "Suivant". Ensuite, soit vous sélectionnez l'option "Tapez un chemin personnalisé" et cliquez sur "Parcourir" pour localiser le dossier que vous souhaitez partager. Une fois que vous avez sélectionné le dossier, cliquez sur "Suivant", soit vous sélectionnez par volume si vous souhaitez créer un nouveau dossier.

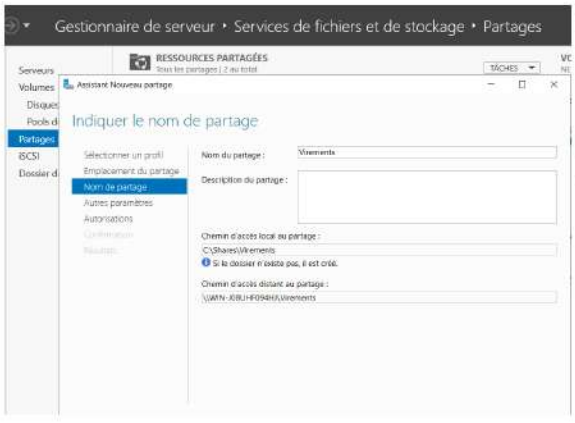
Si nécessaire, vous pouvez modifier le nom du partage, puis cliquez sur "Suivant". Vous avez également la possibilité de modifier les options supplémentaires du partage en fonction de vos besoins. Par exemple, dans le cas d'un dossier confidentiel, il est recommandé de désactiver la mise en cache pour augmenter la sécurité du partage.

Ensuite, cliquez sur "Personnaliser les autorisations" pour modifier les autorisations NTFS et SMB en fonction de vos besoins. Une fois que vous avez configuré les autorisations, cliquez sur "Suivant".

Pour créer le partage, cliquez sur "Créer". Une fois que l'opération est terminée, vous pouvez fermer l'assistant en cliquant sur "Fermer". Le dossier est maintenant partagé et accessible aux utilisateurs autorisés.







Partager un dossier par l'explorateur de fichiers :

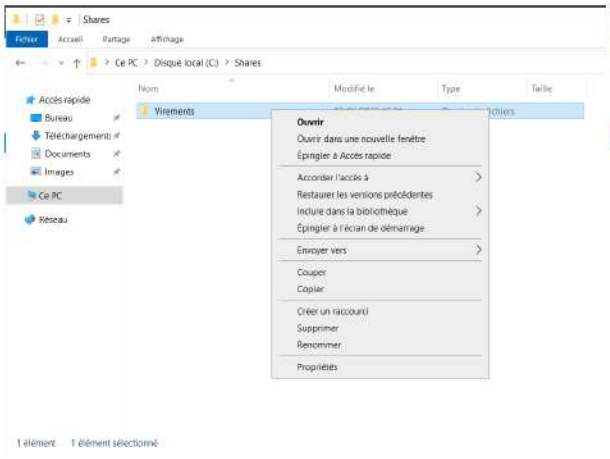
Pour partager un dossier en utilisant l'explorateur de fichiers, vous devez d'abord ouvrir l'explorateur et vous rendre à l'emplacement du dossier que vous souhaitez partager. Ensuite, faites un clic droit sur le dossier et sélectionnez "Propriétés". Dans l'onglet "Partage", cliquez sur "Partage avancé".

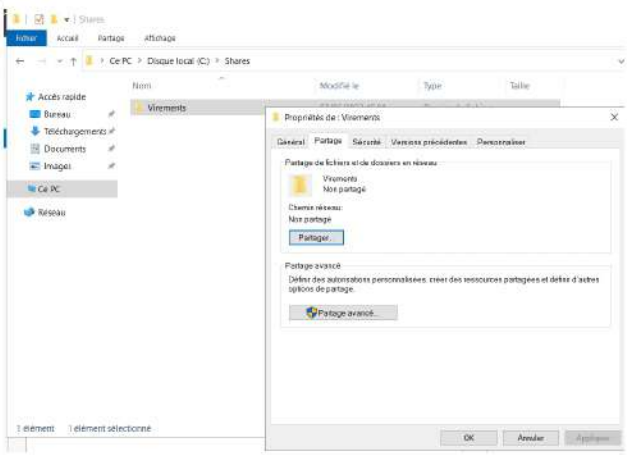
Dans la fenêtre "Partage avancé", cochez la case "Partager ce dossier" et cliquez sur "Autorisations". Vous pouvez maintenant configurer les autorisations de partage en fonction de vos besoins spécifiques. Une fois que vous avez défini les autorisations, cliquez sur "Appliquer" et "OK".

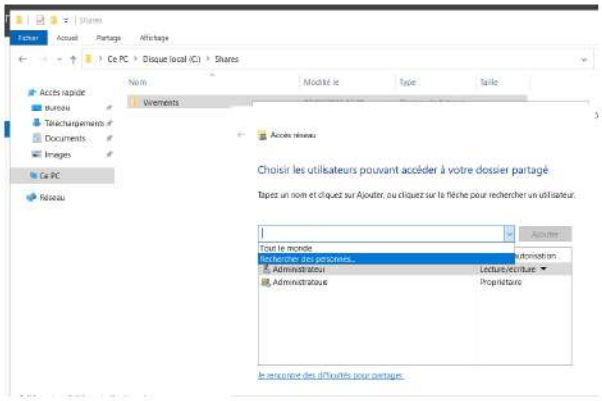
Pour finaliser le partage, cliquez à nouveau sur "Appliquer" et "OK" pour fermer la fenêtre "Partage avancé". À ce stade, le dossier est partagé et vous pouvez voir le chemin d'accès dans les propriétés du dossier.

Pour tester le partage, vous pouvez essayer d'accéder au dossier à partir d'un autre ordinateur en entrant le chemin d'accès dans l'explorateur de fichiers Windows.

Grâce à cette configuration, il est possible de partager un dossier en utilisant l'explorateur de fichiers sur toutes les versions de Windows, que ce soit pour les serveurs ou les ordinateurs de bureau.







Partie 3 : Sécurisation à l'aide de GPO

Gestion de stratégie de groupe (GPO)

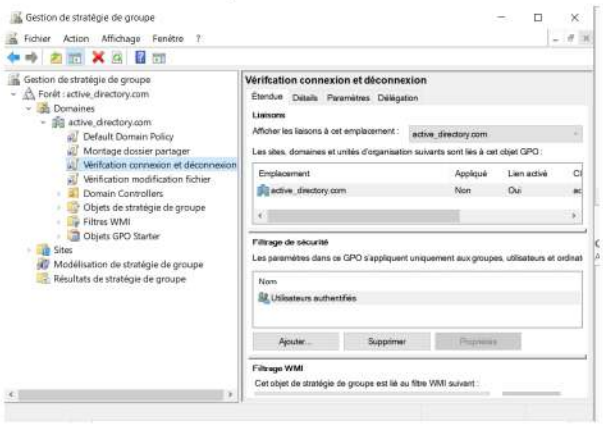
Se connecter au contrôleur de domaine en tant qu'admin ou membre d'un groupe d'admins. Dans l'éditeur de gestion de stratégie de groupe, démarrer puis dans la barre de recherche entrer "gpedit.msc". Cela permet de créer un GPO local sur le contrôleur de domaine.

On peut voir que par défaut, il y une GPO nommée “Default Domain Policy”. Il est préférable de ne pas ajouter de nouvelles stratégies dans cette dernière, mais de créer de nouvelles GPO qui auront un nom explicite sur leurs utilités.

Après avoir fait un clic droit sur la GPO à laquelle on souhaite ajouter des stratégies, on clique sur “Modifier”.

Les GPO dont on parlera permettront d’obtenir les noms des utilisateurs qui se connectent et se déconnectent, d’obtenir le nom des fichiers qui sont modifiés et de mettre en place le lecteur du partage de dossiers.

Voici les 3 GPO qu’on a créées.



"Configuration de l'ordinateur (ou utilisateur)" → "Stratégies" → "Modèles d'administration". De là, sélectionner "Nouveau modèle d'administration", donner un nom au GPO et OK. En ouvrant son éditeur de stratégie, il faut configurer les paramètres qui nous intéressent dans les différentes catégories et sous-catégories. Puis fermer l'éditeur de stratégie de groupe. Attention de lier le GPO à l'OU voulue pour qu'il soit appliqué aux objets cibles.
Dans un objet de stratégie de groupe on peut configurer des paramètres de sécurité comme les MDP, le verrouillage du compte... On peut personnaliser l'apparence et le comportement du bureau. Définir les paramètres du navigateur, ceux du réseau... On peut définir des paramètres spécifiques pour Windows (sécurité Windows, mise à jour Windows...). Configurer des actions au démarrage ou à la fermeture de session des utilisateurs…

Vérification connexion et déconnexion :

Pour pouvoir permettre cela il nécessaire d'activer plusieurs audits sur réussite :
"Configuration ordinateur" → "Stratégies" → "Paramètres Windows" → "Paramètres de sécurité" → "Stratégies locales" → "Stratégie d’audit" :
→ "Auditer les événements de connexion"
→ "Auditer les événements de connexion au compte"

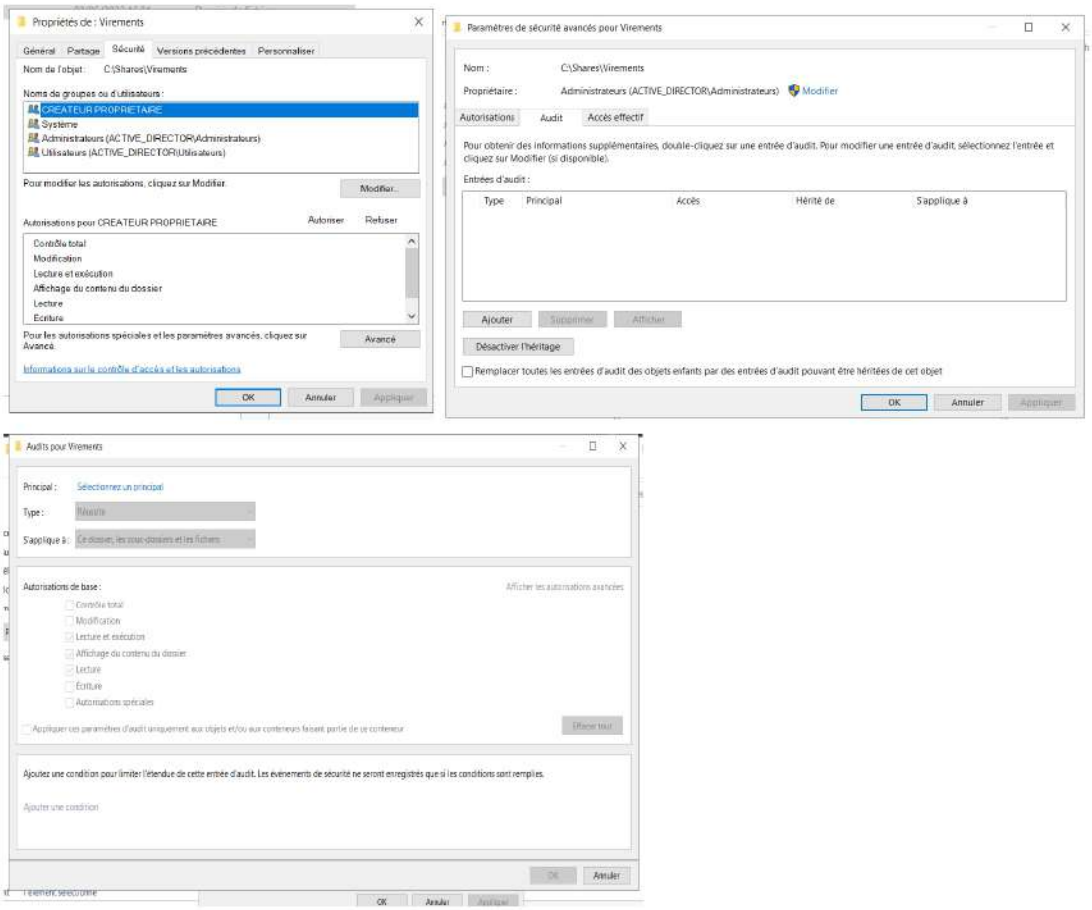
"Configuration ordinateur" → "Stratégies" → "Paramètres Windows" → "Paramètres de sécurité" → "Configuration avancée de la stratégie d'audit" → "Ouvrir/fermer la session" :
→ "Auditer l'ouverture de session"
→ "Auditer la fermeture de session"

Vérification modification fichiers :

Pour pouvoir permettre cela il nécessaire d'activer plusieurs audits sur réussite :
"Configuration ordinateur" → "Stratégies" → "Paramètres Windows" → "Paramètres de sécurité" → "Stratégies locales" → "Stratégie d'audit" :
→ "Auditer l'accès aux objets"
→ "Auditer les événements système"

"Configuration ordinateur" → "Stratégies" → "Paramètres Windows" → "Paramètres de sécurité" → "Configuration avancée de la stratégie d'audit" → "Accès à l'objet" :
→ "Auditer le système de fichiers"

Ensuite il faut activer l'audit sur le dossier que l'on souhaite surveiller. Pour cela, dans l'explorateur de fichier, on va dans propriétés et on y ajoute les utilisateurs ou les groupes qui auront accès aux données de l'audit.



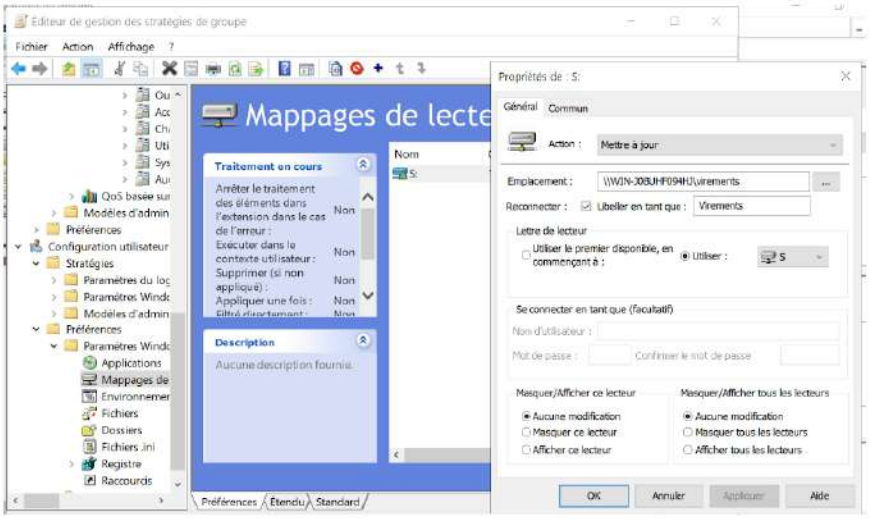
Montage dossier partager :

Pour pouvoir permettre cela il nécessaire d'activer la stratégie :
"Configuration utilisateur" → "Préférences" → "Paramètres Windows" → "Mappages de lecteurs" :
→ "Auditer les événements de connexion"

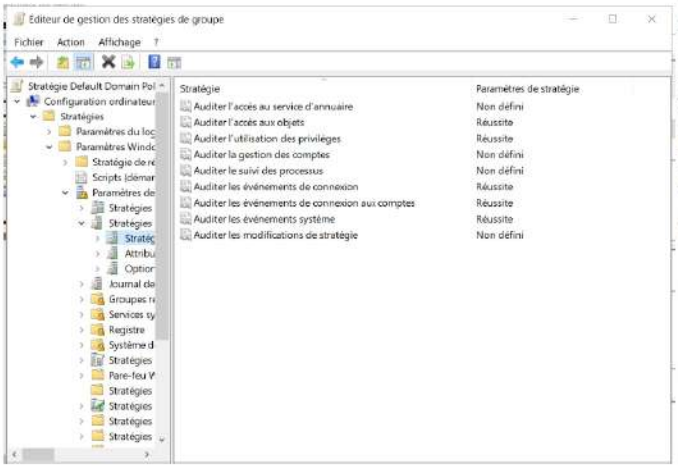
Ensuite effectuer un clic droit, choisir "Nouveau" puis "Lecteur mappé".

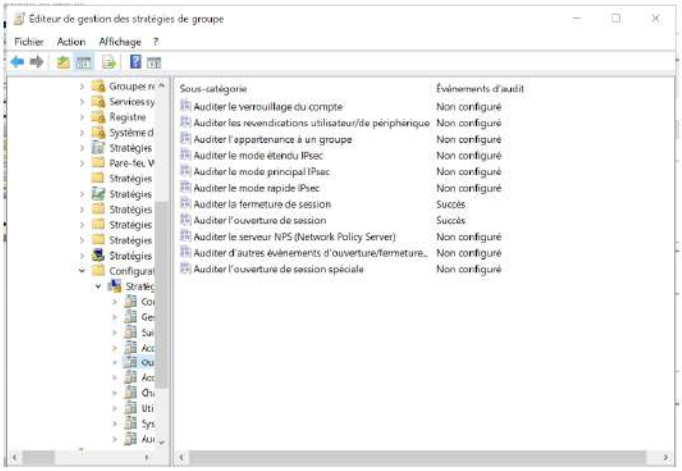
Remplissez le formulaire en spécifiant l'emplacement du partage réseau et la lettre de lecteur à utiliser. Vous pouvez également attribuer un label au lecteur réseau pour faciliter son identification. Une fois les paramètres définis, cliquez sur "Appliquer" et "OK".

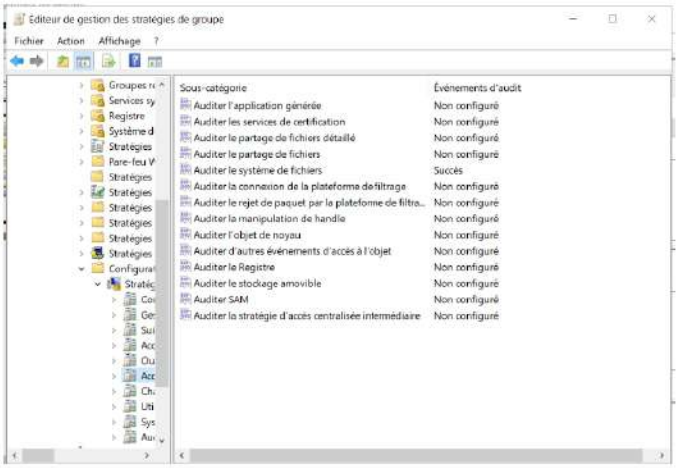
De cette manière, il est possible de configurer une stratégie de groupe pour le mappage de lecteurs réseau. Cela permettra aux utilisateurs de bénéficier d'un accès automatique aux dossiers partagés via un lecteur lorsqu'ils se connectent au domaine.



Voici en résumé tous les audits qu'on a activés



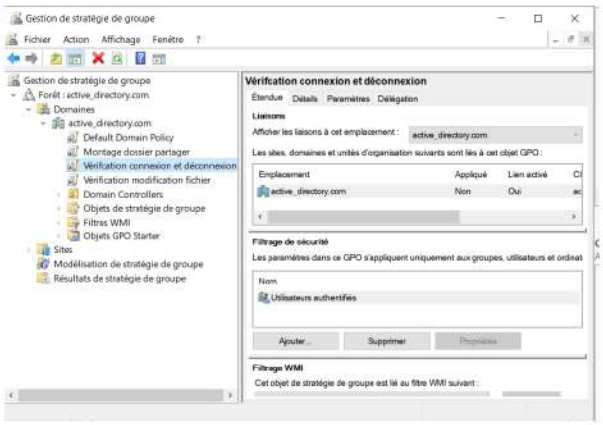




On peut créer ces GPO et les appliquer par défaut à tous les utilisateurs, mais il est préférable de supprimer cette autorisation et ajouter les groupes spécifiques d'utilisateurs.

Limiter une GPO à un groupe :

Pour limiter une GPO à un groupe utilisateurs spécifique, vous devez le ou les ajouter dans la section filtrage de sécurité de la GPO. Cette méthode permet de restreindre l'exécution de la stratégie uniquement aux membres du ou des groupes cibles.



Maintenant que les GPO sont terminées, vous pouvez ouvrir un terminal de commande (cmd) et exécuter la commande **gpupdate /force.**